Effective 5/5/2021

Part 7
Cybersecurity Affirmative Defense Act

78B-4-701 Definitions.

As used in this part:

(1) "Breach of system security" means the same as that term is defined in Section 13-44-102.

(2) "NIST" means the National Institute for Standards and Technology in the United States Department of Commerce.

(3) "PCI data security standard" means the Payment Card Industry Data Security Standard.

(4)

(a) "Person" means:

(i) an individual;

(ii) an association;

(iii) a corporation;

(iv) a joint stock company;

(v) a partnership;

(vi) a business trust; or

(vii) any unincorporated organization.

(b) "Person" includes a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, another state, or another country.

(5) "Personal information" means the same as that term is defined in Section 13-44-102.

Enacted by Chapter 40, 2021 General Session

78B-4-702 Affirmative defense for a breach of system security.

(1) A person that creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4), and is in place at the time of a breach of system security of the person, has an affirmative defense to a claim that:

(a) is brought under the laws of this state or in the courts of this state; and

(b) alleges that the person failed to implement reasonable information security controls that resulted in the breach of system security.

(2) A person has an affirmative defense to a claim that the person failed to appropriately respond to a breach of system security if:

(a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4) and is in place at the time of the breach of system security; and

(b) the written cybersecurity program had protocols at the time of the breach of system security for responding to a breach of system security that reasonably complied with the written cybersecurity program under Subsection (2)(a) and the person followed the protocols.

(3) A person has an affirmative defense to a claim that the person failed to appropriately notify an individual whose personal information was compromised in a breach of system security if:

(a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4) and is in place at the time of the breach of system security; and

(b) the written cybersecurity program had protocols at the time of the breach of system security for notifying an individual about a breach of system security that reasonably complied with

the requirements for a written cybersecurity program under Subsection (3)(a) and the person followed the protocols.

(4) A written cybersecurity program described in Subsections (1), (2), and (3) shall provide administrative, technical, and physical safeguards to protect personal information, including:

(a) being designed to:

(i) protect the security, confidentiality, and integrity of personal information;

(ii) protect against any anticipated threat or hazard to the security, confidentiality, or integrity of personal information; and

(iii) protect against a breach of system security;

(b) reasonably conforming to a recognized cybersecurity framework as described in Subsection 78B-4-703(1); and

(c) being of an appropriate scale and scope in light of the following factors:

(i) the size and complexity of the person;

(ii) the nature and scope of the activities of the person;

(iii) the sensitivity of the information to be protected;

(iv) the cost and availability of tools to improve information security and reduce vulnerability; and

(v) the resources available to the person.

(5)

(a) Subject to Subsection (5)(b), a person may not claim an affirmative defense under Subsection (1), (2), or (3) if:

(i) the person had actual notice of a threat or hazard to the security, confidentiality, or integrity of personal information;

(ii) the person did not act in a reasonable amount of time to take known remedial efforts to protect the personal information against the threat or hazard; and

(iii) the threat or hazard resulted in the breach of system security.

(b) A risk assessment to improve the security, confidentiality, or integrity of personal information is not an actual notice of a threat or hazard to the security, confidentiality, or integrity of personal information.

Enacted by Chapter 40, 2021 General Session

78B-4-703 Components of a cybersecurity program eligible for an affirmative defense.

(1) Subject to Subsection (3), a person's written cybersecurity program reasonably conforms to a recognized cybersecurity framework if the written cybersecurity program:

(a) is designed to protect the type of personal information obtained in the breach of system security; and

(b)

(i) is a reasonable security program described in Subsection (2);

(ii) reasonably conforms to the current version of any of the following frameworks or publications, or any combination of the following frameworks or publications:

(A) NIST special publication 800-171;

(B) NIST special publications 800-53 and 800-53a;

(C) the Federal Risk and Authorization Management Program Security Assessment Framework;

(D) the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or

(E) the International Organization for Standardization/International Electrotechnical Commission 27000 Family - Information security management systems;

(iii) for personal information obtained in the breach of the system security that is regulated by the federal government or state government, reasonably complies with the requirements of the regulation, including:
(A) the security requirements of the Health Insurance Portability and Accountability Act of 1996, as described in 45 C.F.R. Part 164, Subpart C;
(B) Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended;
(C) the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283;
(D) the Health Information Technology for Economic and Clinical Health Act, as provided in 45 C.F.R. Part 164;
(E)Title 13, Chapter 44, Protection of Personal Information Act; or
(F) any other applicable federal or state regulation; or
(iv) for personal information obtained in the breach of system security that is the type of information intended to be protected by the PCI data security standard, reasonably complies with the current version of the PCI data security standard.

(2) A written cybersecurity program is a reasonable security program under Subsection (1)(b)(i) if:
(a) the person coordinates, or designates an employee of the person to coordinate, a program that provides the administrative, technical, and physical safeguards described in Subsections 78B-4-702(4)(a) and (c);
(b) the program under Subsection (2)(a) has practices and procedures to detect, prevent, and respond to a breach of system security;
(c) the person, or an employee of the person, trains, and manages employees in the practices and procedures under Subsection (2)(b);
(d) the person, or an employee of the person, conducts risk assessments to test and monitor the practice and procedures under Subsection (2)(b), including risk assessments on:
(i) the network and software design for the person;
(ii) information processing, transmission, and storage of personal information; and
(iii) the storage and disposal of personal information; and
(e) the person adjusts the practices and procedures under Subsection (2)(b) in light of changes or new circumstances needed to protect the security, confidentiality, and integrity of personal information.

(3)
(a) If a recognized cybersecurity framework described in Subsection (1)(b)(ii) or (iv) is revised, a person with a written cybersecurity program that relies upon that recognized cybersecurity framework shall reasonably conform to the revised version of the framework no later than one year after the day in which the revised version of the framework is published.
(b) If a recognized cybersecurity framework described in Subsection (1)(b)(iii) is amended, a person with a written cybersecurity program that relies upon that recognized cybersecurity framework shall reasonably conform to the amended regulation of the framework in a reasonable amount of time, taking into consideration the urgency of the amendment in terms of:
(i) risks to the security of personal information;
(ii) the cost and effort of complying with the amended regulation; and
(iii) any other relevant factor.

Enacted by Chapter 40, 2021 General Session

78B-4-704 No cause of action.

This part may not be construed to create a private cause of action, including a class action, if a person fails to comply with a provision of this part.

Enacted by Chapter 40, 2021 General Session

78B-4-705 Choice of law.

A choice of law provision in an agreement that designates this state as the governing law shall apply this part, if applicable, to the fullest extent possible in a civil action brought against a person regardless of whether the civil action is brought in this state or another state.

Enacted by Chapter 40, 2021 General Session

78B-4-706 Severability clause.

If any provision of this part, or the application of any provision of this part to any person or circumstance, is held invalid, the remainder of this part shall be given effect without the invalid provision or application.

Enacted by Chapter 40, 2021 General Session